

POLITICA PER LA SECURITY

La Direzione di Consafety, consapevole dell'importanza e della necessità di avvalersi di un Sistema di Gestione per la Sicurezza delle Informazioni riconosciuto in ambito internazionale, al fine di garantire la qualità dei servizi forniti e perseguire la soddisfazione dei propri Clienti, ritiene opportuno mantenere il proprio Sistema di Gestione Sicurezza delle Informazioni conforme allo standard ISO/IEC 27001, aggiornato all'ultima edizione in vigore.

Obiettivi primari della presente politica di sicurezza delle informazioni aziendali sono i seguenti:

- Assegnare la responsabilità di tenuta sotto controllo degli asset aziendali al personale in modo che tutti, nelle modalità pertinenti al proprio ruolo e funzione, siano coinvolti e partecipi nella difesa del patrimonio delle informazioni di Consafety;
- Stabilire modalità di controllo per il trasferimento all'esterno di asset aziendali;
- Assicurare che nell'alienazione di qualunque asset aziendale non si verifichi perdita in termini di riservatezza delle informazioni eventualmente in esso contenute;
- Attuare tutte le azioni possibili al fine di preservare l'integrità, la disponibilità e la riservatezza di qualunque asset appartenente a Consafety, a clienti e fornitori;
- Mettere a disposizione le risorse necessarie al fine di perseguire il miglioramento continuo sfruttando nel miglior modo possibile le potenzialità offerte dall'applicazione del sistema di gestione ISO 27001;
- Valutare periodicamente il grado di conformità rispetto agli adempimenti cogenti applicabili al contesto dell'organizzazione;
- Tutelare la privacy proteggendo tutti i dati personali, con particolare attenzione a quelli di proprietà di clienti, fornitori e altre parti interessate;
- Analizzare le cause di incidenti informatici, al fine di imparare da errori e attuare le necessarie azioni correttive per evitare che si verifichino di nuovo;
- Controllare gli accessi dei visitatori negli uffici aziendali e tutti gli accessi a qualsivoglia informazione aziendale effettuata dal Personale o da terzi a vario titolo;
- Verificare che tutte le postazioni di lavoro abbiano accesso protetto da password periodicamente modificate;
- Definire e testare periodicamente procedure di back-up efficaci;
- Stabilire con i clienti e con i fornitori responsabilità reciproche nella gestione della sicurezza delle informazioni;
- Verificare periodicamente l'efficacia del piano di business continuity e disaster recovery;

- Stabilire le buone prassi dal punto di vista di sicurezza delle informazioni per lo smart working e controllare il rispetto delle policy condivise da parte di tutti i dipendenti e collaboratori di Consafety.

Tutto il Personale, i collaboratori, i fornitori, i visitatori, dovranno operare nel rispetto delle norme e delle procedure aziendali predisposte al fine di assicurare la gestione del business aziendale in conformità ai predetti principi.

La Direzione si augura di ottenere, a tutti i livelli, la massima collaborazione per il rispetto e la sistematica applicazione di tali linee di indirizzo generali.

Roma li, 26/01/2026



Rappresentante Legale
Giuseppina Zippo